BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen: 102 56 586.4

Anmeldetag: 04. Dezember 2002

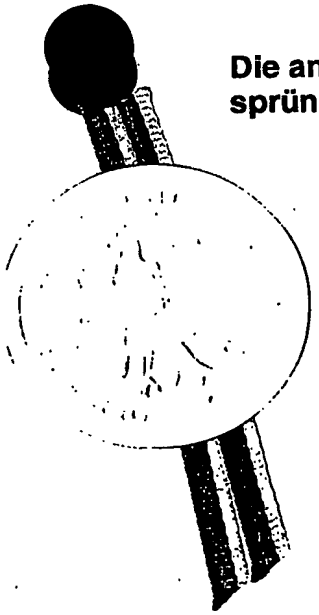
Anmelder/Inhaber: Philips Intellectual Property & Standards GmbH, Hamburg/DE

(vormals: Philips Corporate Intellectual Property GmbH)

Bezeichnung: Datenverarbeitungseinrichtung mit Mikroprozessor und mit zusätzlicher Recheneinheit sowie zugeordnetes Verfahren

IPC: G 06 F 17/00

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.



München, den 16. Oktober 2003
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Faust

A 9161
08/00
EDV-L

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

BESCHREIBUNG

Datenverarbeitungseinrichtung mit Mikroprozessor und mit zusätzlicher Recheneinheit sowie zugeordnetes Verfahren

Die vorliegende Erfindung betrifft eine Datenverarbeitungseinrichtung mit mindestens einem Mikroprozessor und mit mindestens einer zusätzlichen Recheneinheit sowie ein Verfahren zum Durchführen mindestens einer bestimmten festgelegten Berechnung mittels mindestens einer Datenverarbeitungseinrichtung der vorgenannten Art.

Derartige, insbesondere in einem einzigen Halbleiterchip integrierte Datenverarbeitungseinrichtungen sind grundsätzlich bekannt, beispielsweise aus dem Datenblatt zur integrierten Schaltung mit der Bezeichnung P83C852 von Philips.

Diese integrierte Schaltung wird unter anderem in tragbare kartenförmige Datenträger, zum Beispiel in Datenträger mit dem Format einer Scheckkarte, eingebaut und dient etwa dazu, Daten nach einem unsymmetrischen Verschlüsselungsverfahren zu verschlüsseln oder derartige Daten zu entschlüsseln. Dabei sind unter anderem Datenblöcke mit einer Schlüsselzahl modulo einer Konstanten zu potenzieren, wobei die Konstante eine hohe Stellenzahl aufweist, um eine möglichst sichere Verschlüsselung zu erreichen.

Die hierfür erforderlichen Rechenschritte können grundsätzlich auch mittels des Mikroprozessors durchgeführt werden; dies würde jedoch eine zu lange Zeit erfordern, so dass zusätzlich zum Mikroprozessor eine spezielle Recheneinheit auf dem Chip integriert ist, die für die zum Verschlüsseln erforderlichen Rechenschritte optimal ausgelegt ist. Die Verbindung zwischen Mikroprozessor und zusätzlicher Recheneinheit erfolgt in diesem Zusammenhang über besondere, die Datenübertragung steuernde Register sowie über mindestens einen Datenspeicher, auf den sowohl der Mikroprozessor als auch die zusätzliche Recheneinheit zugreifen.

Nachteilig bei diesen bekannten integrierten Schaltungen mit Mikroprozessor und mit zusätzlicher Recheneinheit ist es, dass nach Durchführen eines Verarbeitungsschritts oder eines Verarbeitungszyklusses durch die zusätzliche Recheneinheit der Mikroprozessor die Register wieder mit neuen Werten für zumindest zum Teil neue Operanden laden muss, mit denen dann der nächste Verarbeitungszyklus startet. Dies bedingt einen erheblichen Zeitverlust, so dass die gesamte Datenverarbeitungseinrichtung insbesondere bei längeren Schlüsselzahlen zu viel Zeit für die Datenverschlüsselung bzw. Datenentschlüsselung benötigt.

Damit nun die Recheneinheit nach Abschluss eines Verarbeitungszyklusses möglichst ohne Zeitverlust sofort mit dem nächsten Verarbeitungszyklus für neue Daten beginnen kann, werden gemäß der Offenbarung der Druckschrift EP 0 822 482 A2 die Register zum Steuern der Datenübertragung und zum Übertragen von Befehlen als mindestens zwei Sätze von Registern vorgesehen.

In diesem Zusammenhang werden die Ausgänge dieser Register durch den Inhalt eines weiteren Registers umgeschaltet, so dass jeweils nur ein Satz von Registern wirksam ist. In die nicht wirksamen Register können jedoch jederzeit vom Mikroprozessor neue Daten eingeschrieben werden, so dass diese Daten bereitstehen, wenn die Recheneinheit einen Verarbeitungszyklus abgeschlossen hat, und sofort mit dem nächsten Verarbeitungszyklus begonnen werden kann; hierdurch wird ein Verschlüsselungs- bzw. Entschlüsselungsvorgang erheblich beschleunigt.

Gemäß der Offenbarung der Druckschrift EP 0 822 482 A2 kann die Initialisierung der Recheneinheit C durch mehrere parallele Registersätze R1, R2, R3, R4, R5 und durch eine Auswahlschaltung S beschleunigt werden. Hierdurch können die Register während einer Berechnung für die folgende Berechnung geladen werden (vgl. Figur 1, in der ein Blockschaltbild der gemäß der Druckschrift EP 0 822 482 A2 aufgebauten Datenverarbeitungseinrichtung D, bei der die Recheneinheit C durch drei Sätze a, b, c von Registern R1, R2, R3, R4, R5 gesteuert wird, schematisch dargestellt ist; das Bezugszeichen K bezeichnet das Kontrollregister).

Das jeweils aktive Register stellt für die Recheneinheit die Eingabewerte bereit und darf während der Berechnung nicht verändert werden. Ein Modifizieren dieses Registersatzes ist somit erst bei der folgenden Berechnung mit einem anderen Registersatz oder in einer Pause zwischen zwei Berechnungen möglich.

Der Nachteil bei der Implementierung gemäß der Druckschrift EP 0 822 482 A2 besteht darin, dass jeder zusätzliche Registersatz Chipfläche verbraucht, und zwar in Abhängigkeit von der Größe eines Registersatzes. Moderne kryptographische Algorithmen setzen sich oftmals aus einer Vielzahl kleiner schneller Operationen zusammen, wodurch eine große Anzahl an Registersätzen benötigt wird, um eine schnelle Berechnung zu ermöglichen.

Des weiteren muss gemäß dem Stand der Technik der Mikroprozessor jede einzelne Berechnung durch Setzen eines entsprechenden Kontrollbits starten, wodurch eine weitere Verzögerung erfolgen kann.

Ausgehend von den vorstehend dargelegten Nachteilen und Unzulänglichkeiten sowie unter Würdigung des umrissenen Standes der Technik liegt der vorliegenden Erfindung die Aufgabe zugrunde, eine Datenverarbeitungseinrichtung der eingangs genannten Art (vgl. Druckschrift EP 0 822 482 A2 aus dem Stand der Technik) sowie ein Verfahren der eingangs genannten Art so weiterzuentwickeln, dass eine Vielzahl von Berechnungen in Folge ohne Eingreifen des Mikroprozessors durchgeführt werden kann.

Diese Aufgabe wird durch eine Datenverarbeitungseinrichtung mit den im Anspruch 1 angegebenen Merkmalen sowie durch ein Verfahren mit den im Anspruch 10 angegebenen Merkmalen gelöst. Vorteilhafte Ausgestaltungen und zweckmäßige Weiterbildungen der vorliegenden Erfindung sind in den Unteransprüchen gekennzeichnet.

Gemäß der Lehre der vorliegenden Erfindung werden die Register zur Steuerung der Datenübertragung und zur Befehlsübertragung aus mindestens einem peripheren Speicher, zum Beispiel aus mindestens einem R[andom]A[ccess]M[emory]-Speicher, aus mindestens einem R[ead]O[nly]M[emory]-Speicher oder aus mindestens einem

E[lectrical] E[rasable]P[rogrammable]R[ead]O[nly]M[emory]-Speicher, geladen. Mithin ist erfindungsgemäß ein gleichsam automatisches Laden von Eingangsdatensätzen für einen Mikroprozessor mit zusätzlicher Recheneinheit vorgeschlagen.

Gemäß einer besonders erfinderischen Weiterbildung ist dem Speicher mindestens ein zusätzliches, mit mindestens einer Kontrolllogik in Verbindung stehendes Adressregister zugeordnet, das in bezug auf das Laden der Register als Zeiger auf die Startadresse der zu ladenden Daten dient. In bevorzugter Weise gibt mindestens ein ebenfalls mit der Kontrolllogik in Verbindung stehendes Zählregister die in Folge zu ladenden Registersätze an.

Da das Nachladen aus dem insbesondere peripheren Speicher in aller Regel schneller als das Laden der Register über den Mikroprozessor ist, lässt sich erfindungsgemäß eine große Anzahl von Operationen in Folge ohne Zeitverlust zwischen den Berechnungen durchführen. Dies korrespondiert erfindungsgemäß damit, dass die Eingaberegister vor und während der Berechnung geladen werden, indem Daten vom angesprochenen Speicher geholt bzw. geladen werden.

Da für die gesamte Berechnung (= x Einzelberechnungen) lediglich das Adressregister und das Zählregister initialisiert werden, ist die Codegröße des Mikroprozessors im Vergleich zur aus dem Stand der Technik bekannten Lösung mit mehreren Registersätzen deutlich kleiner. Die Registerdaten können zum Beispiel als Rohdaten im Programmcode des Mikroprozessors abgelegt werden.

Die vorstehend beschriebene Datenverarbeitungseinrichtung mit mindestens einem Mikroprozessor und mit mindestens einer zusätzlichen Recheneinheit dient zum Durchführen bestimmter festgelegter Berechnungen, was nach den folgenden Verfahrensschritten gemäß der vorliegenden Erfindung erfolgt:

Zunächst werden die beiden zusätzlichen Register, das heißt das Adressregister und das Zählregister, durch den Mikroprozessor initialisiert, und die Berechnung durch Setzen eines Kontrollbits kann starten. Beginnend bei der durch das Register angegebenen Startadresse werden die Daten aus dem peripheren Speicher in einen temporären Registersatz geladen. Das Adressregister wird hierbei mit jedem Zugriff auf den Speicher um eins inkrementiert.

Ist der temporäre Registersatz voll(ständig), so wird dieser temporäre Registersatz in den Hauptregistersatz übertragen und sodann das Zählregister um eins reduziert, und die zusätzliche Recheneinheit beginnt mit der eigentlichen Berechnung. Während dieser Berechnung wird der nächstfolgende Registersatz aus dem Speicher in den temporären Registersatz gespeichert.

Ist die laufende Berechnung beendet, so wird der temporäre Registersatz in den Hauptregistersatz gespeichert, das Zählregister um eins reduziert und sofort die nächste Berechnung gestartet, ohne dass der Mikroprozessor in irgendeiner Art und Weise eingreifen muss. Dieser Vorgang wiederholt sich, bis das Zählregister auf Null dekrementiert ist.

Gemäß einer bevorzugten Weiterbildung der vorliegenden Erfindung kann zwischen dem temporären Registersatz und dem Hauptregistersatz mindestens eine Auswahlschaltung geschaltet sein, so dass die hier beschriebene Erfindung problemlos mit einer mehrere Sätze von dem Mikroprozessor zugeordneten Registern aufweisenden Ausgestaltung kombiniert werden kann. Durch die Verwendung des Hauptregistersatzes, in dem die Register für die aktive Berechung gespeichert werden, kann der aktive Registersatz nach dem Starten der Berechnung für die nachfolgende Berechnung modifiziert werden.

Als Quelle für die zu ladenden Registerdaten kann in zweckmäßiger Weise jeder adressierbare Speicher dienen (, wobei jedoch auf Konflikte beim Speicherzugriff anderer Schaltungsblöcke, zum Beispiel des Mikroprozessors, zu achten ist). Das Vorsehen mindestens eines M[emory]M[anagement]S[ystems] bzw. mindestens einer M[emory] M[anagement]U[nit] kann hierbei parallele Zugriffe auf einen Speicher regeln.

Unabhängig hiervon oder in Verbindung hiermit bietet sich des weiteren die erfindungswesentliche Option eines universellen Adresszeigers an, mit dessen Hilfe auf mehrere Speicherblöcke zugegriffen werden kann. Diese zusätzliche Sonderfunktion eignet sich vor allem für das zuvor beschriebene Adressregister gemäß der vorliegenden Erfindung.

Die vorliegende Erfindung betrifft des weiteren einen tragbaren Datenträger mit mindestens einer Datenverarbeitungseinrichtung gemäß der vorstehend dargelegten Art.

Die vorliegende Erfindung betrifft schließlich einen Halbleiterchip mit mindestens einer integrierten Datenverarbeitungseinrichtung gemäß der vorstehend dargelegten Art.

Wie bereits vorstehend erörtert, gibt es verschiedene Möglichkeiten, die Lehre der vorliegenden Erfindung in vorteilhafter Weise auszugestalten und weiterzubilden. Hierzu wird einerseits auf die dem Anspruch 1 nachgeordneten Ansprüche verwiesen, andererseits werden weitere Ausgestaltungen, Merkmale und Vorteile der vorliegenden Erfindung nachstehend anhand der beiden durch die Figuren 2 bis 5 veranschaulichten Ausführungsbeispiele näher erläutert.

Es zeigt:

Fig. 1 in schematischer Darstellung ein Blockschaltbild einer Datenverarbeitungseinrichtung, bei der die Recheneinheit durch drei Sätze von Registern gesteuert wird, gemäß dem Stand der Technik;

Fig. 2 in schematischer Darstellung ein Blockschaltbild eines ersten Ausführungsbeispiels einer Datenverarbeitungseinrichtung gemäß der vorliegenden Erfindung;

Fig. 3 in schematischer Darstellung ein Ablaufdiagramm für ein der Datenverarbeitungseinrichtung aus Fig. 2 zugeordnetes Verfahren zum Durchführen bestimmter festgelegter Berechnungen;

Fig. 4 in schematischer Darstellung ein Blockschaltbild eines zweiten Ausführungsbeispiels einer Datenverarbeitungseinrichtung, bei der die Recheneinheit durch drei Sätze von Registern gesteuert wird, gemäß der vorliegenden Erfindung; und

Fig. 5 in schematischer Übersichtsdarstellung ein Blockschaltbild der gesamten Datenverarbeitungseinrichtung gemäß der vorliegenden Erfindung in Form einer vereinfachenden Zusammenschau des ersten Ausführungsbeispiels aus Fig. 2 und des zweiten Ausführungsbeispiels aus Fig. 4.

Gleiche oder ähnliche Ausgestaltungen, Elemente oder Merkmale sind in den Figuren 2 bis 5 mit identischen Bezugszeichen versehen.

In Figur 2 dargestellt ist ein erstes Ausführungsbeispiel für eine Datenverarbeitungseinrichtung 100 mit Mikroprozessor 90 und mit zusätzlicher spezieller Recheneinheit 40 für bestimmte Berechnungen, deren Durchführung mittels des Mikroprozessors 90 zeitlich zu aufwendig wäre.

Die Recheneinheit 40 ist mit dem Mikroprozessor 90 über eine Anzahl von Registern gekoppelt, von denen grundsätzlich erste Register zum Steuern der Datenübertragung und zweite Register zum Übertragen von Befehlen vorgesehen sind. Des weiteren ist der Recheneinheit 40 ein Kontrollregister 50 zugeordnet, das mit der Kontrolllogik 60 in Verbindung 560 steht.

Die Besonderheit der Datenverarbeitungseinrichtung 100 gemäß dem ersten Ausführungsbeispiel ist unter anderem darin zu sehen, dass die Register aus einem peripheren Speicher 10 in Form eines E[lectrical]E[rasable]P[rogrammable]R[ead]O[nly]M[emory]-Speichers ladbar sind. Mithin ist ein automatisches Laden von Eingangsdatensätzen für den Mikroprozessor 90 mit zusätzlicher Recheneinheit 40 gegeben.

Wie der Darstellung der Figur 2 ferner entnehmbar ist, ist dem peripheren Speicher 10 ein zusätzliches, mit einer Kontrolllogik 60 in Verbindung 670 stehendes Adressregister 70 zugeordnet, das in bezug auf das Laden der Register als Zeiger auf die Startadresse der zu ladenden Daten dient, so dass der Speicher 10 durch das Adressregister 70 beaufschlagbar ist (--> Bezugszeichen 170). Des weiteren gibt ein ebenfalls mit der Kontrolllogik 60 in Verbindung 672 stehendes Zählregister 72 die in Folge zu ladenden Registersätze an und definiert die Anzahl der Berechnungen.

Was nun eine genauere Beschreibung der Register anbelangt, so ist dem Speicher 10 ein Satz von fünf temporären Registern 20, 22, 24, 26, 28 zugeordnet, der mit einem der Recheneinheit 40 zugeordneten, zum Speichern der Register für die aktive Berechnung bestimmten Satz von fünf Hauptregistern 30, 32, 34, 36, 38 in jeweiliger Verbindung 230, 232, 234, 236, 238 steht.

Da das Nachladen aus dem Speicher 10 in aller Regel schneller als das Laden der Register über den Mikroprozessor 90 ist, lässt sich mit der Datenverarbeitungseinrichtung 100 gemäß dem ersten Ausführungsbeispiel eine große Anzahl von Operationen in Folge ohne Zeitverlust zwischen den Berechnungen durchführen. Da für die gesamte Berechnung (= x Einzelberechnungen) lediglich das Adressregister 70 und das Zählregister 72 initialisiert werden, ist die Codegröße des Mikroprozessors 90 relativ klein. Die Registerdaten können zum Beispiel als Rohdaten im Programmcode des Mikroprozessors 90 abgelegt werden.

Im einzelnen arbeitet die vorstehend beschriebene Datenverarbeitungseinrichtung 100 beim Durchführen der bestimmten festgelegten Berechnungen gemäß den folgenden, anhand Figur 3 veranschaulichten Verfahrensschritten:

(i) zunächst werden die beiden zusätzlichen Register, das heißt das Adressregister 70 und das Zählregister 72, durch den Mikroprozessor 90 initialisiert;

(ii) dann kann die Berechnung durch Setzen eines Kontrollbits starten;

(iii) beginnend bei der durch das Register angegebenen Startadresse werden die Daten aus dem peripheren Speicher 10 über einen internen Datenbus 120 in einen Satz temporärer Register 20, 22, 24, 26, 28 geladen,

(iv) wobei das Adressregister 70 mit jedem Zugriff auf den Speicher 10 um eins inkrementiert wird;

(v.a) ist der Satz temporärer Register 20, 22, 24, 26, 28 voll(ständig) und

(vi.b) ist die Recheneinheit 40 nicht aktiv,

(vii) so wird der Satz temporärer Register 20, 22, 24, 26, 28 in den Satz von Hauptregistern 30, 32, 34, 36, 38 übertragen und

(viii) sodann das Zählregister 72 um eins reduziert, und

(ix) die zusätzliche Recheneinheit 40 beginnt mit der eigentlichen Berechnung; während dieser Berechnung wird der nächstfolgende Registersatz aus dem Speicher 10 in den Satz temporärer Register 20, 22, 24, 26, 28 gespeichert; ist die laufende Berechnung beendet, so wird der Satz temporärer Register 20, 22, 24, 26, 28 in den Satz von Hauptregistern 30, 32, 34, 36, 38 gespeichert, das Zählregister 72 um eins reduziert und sofort die nächste Berechnung gestartet, ohne dass der Mikroprozessor 90 in irgendeiner Art und Weise eingreifen muss;

(x) dieser Vorgang wiederholt sich, bis das Zählregister 72 auf Null dekrementiert ist,

(xi) woraufhin beendet wird.

Das zweite Ausführungsbeispiel für eine Datenverarbeitungseinrichtung 100' gemäß Figur 4 unterscheidet sich vom ersten Ausführungsbeispiel für eine Datenverarbeitungseinrichtung 100 gemäß Figur 2 im wesentlichen dadurch, dass zwischen den Satz temporärer Register 20, 22, 24, 26, 28 und den Satz von Hauptregistern 30, 32, 34, 36, 38 eine Auswahlschaltung 74 geschaltet ist, die durch Bitstellen 51, 52, 53, 54 des Kontrollregisters 50 beaufschlagbar ist.

Mithin kann das in Figur 2 dargestellte erste Ausführungsbeispiel einer Datenverarbeitungseinrichtung 100 durch Verwendung mindestens eines Eingabemultiplexers mit drei Sätzen a, b, c von jeweils fünf Registern 80, 82, 84, 86, 88 erweitert bzw. kombiniert

werden, wobei diese Registersätze 80a, 80b, 80c, 82a, 82b, 82c, 84a, 84b, 84c, 86a, 86b, 86c, 88a, 88b, 88c ihre Daten über einen Datenbus 980 vom Mikroprozessor 90 beziehen, wohingegen zur Steuerung der Recheneinheit 40 durch die schematisch dargestellten Register ein Satz von fünf temporären Registern 20, 22, 24, 26, 28 seine jeweiligen Daten über den Datenbus 120 vom Speicher 10 bezieht.

Die Ausgänge aller Register führen auf die Auswahlschaltung 74, die die Ausgänge von einem dieser Sätze von Registern auswählt und über den Satz von fünf Hauptregistern 30, 32, 34, 36, 38 der Recheneinheit 40 zuführt, wobei die Auswahl durch eine auf den über den internen Datenbus 120 mit Daten vom Speicher 10 versorgten temporären Registersatz 20, 22, 24, 26, 28 bezogene Bitstelle 51 bzw. durch drei auf die drei über den internen Datenbus 980 mit Daten vom Mikroprozessor 90 versorgten Registersätze 80a, 80b, 80c, 82a, 82b, 82c, 84a, 84b, 84c, 86a, 86b, 86c, 88a, 88b, 88c bezogene Bitstellen 52, 53, 54 des nur einmal vorhandenen Kontrollregisters 50 gesteuert wird.

Die Eingänge aller Register sind an einen im wesentlichen nur zum Übertragen von Daten bestimmten internen Datenbus angeschlossen und können vom Mikroprozessor 90 einzeln zum Schreiben ausgewählt werden, wobei die Auswahlleitungen der Übersichtlichkeit halber weggelassen sind.

Die Register 80a, 80b, 80c, 82a, 82b, 82c, 84a, 84b, 84c, 86a, 86b, 86c, 88a, 88b, 88c können je ein Byte Daten nur vom internen Bus aufnehmen und nur an die Auswahlschaltung 40 abgeben, während das Kontrollregister 50 bitweise schreibbar und lesbar ist, wobei die Bitstellen 51, 52, 53, 54, 55 nur vom internen Datenbus Daten übernehmen und über die Ausgänge die Auswahlschaltung 74 (--> Bitstellen 51, 52, 53, 54) sowie die Recheneinheit 40 (--> Bitstelle 55) steuern, während die Bitstellen 56, 57, 58, 59 für weitere Kommunikation zwischen der Recheneinheit 40 und dem Mikroprozessor 90 vorgesehen sind.

Abschließend ist nun in Figur 5 in schematischer Übersichtsdarstellung ein Blockschaltbild einer gesamten Datenverarbeitungseinrichtung 100, 100' gemäß der vorliegenden Erfindung in Form einer vereinigenden Zusammenschau aus dem ersten Ausführungsbeispiel (Datenverarbeitungseinrichtung 100 gemäß Figur 2) und dem zweiten Ausführungsbeispiel (Datenverarbeitungseinrichtung 100' gemäß Figur 4) gezeigt.

Die Gesamt-Datenverarbeitungseinrichtung 100, 100' enthält unter anderem den Mikroprozessor 90 sowie die zusätzliche spezielle Recheneinheit 40 für bestimmte Berechnungen, deren Durchführung mittels des Mikroprozessors 90 zeitlich zu aufwendig wäre.

Ferner sind in der Gesamt-Datenverarbeitungseinrichtung 100, 100' ein flüchtiger Speicher 16 sowie ein erster Schreib-/Lese-Speicher 76 und ein zweiter Schreib-/Lese-Speicher 78 vorgesehen. Der Mikroprozessor 90 ist mit den beiden Schreib-/Lese-Speichern 76, 78 im wesentlichen direkt über den vorbeschriebenen (vgl. Figur 4) internen Bus 980 gekoppelt. Des weiteren ist

- der Mikroprozessor 90 über weitere Adressregister 14 mit dem flüchtigen Speicher 16 sowie
- der periphere Speicher 10 über weitere Register 12 mit der Recheneinheit 40

gekoppelt.

Zwar ist die Steuerung der zusätzlichen Recheneinheit 40 durch die in Figur 5 schematisch dargestellten weiteren Register 12 in der Beschreibung zu den Figuren 2, 3 und 4 deutlicher und im Detail erläutert, jedoch sei an dieser Stelle kurz ergänzt, dass über die weiteren Register 12 im wesentlichen Steuersignale zum Steuern der Funktion der zusätzlichen Recheneinheit 40 sowie zum Steuern der Übertragung von Operanden für die Recheneinheit 40 und von Ergebnissen von der Recheneinheit 40 übertragen werden.

Die Operanden selbst werden über Operandenregister 42, 44, 46 an die Recheneinheit 40 übertragen, das von der Recheneinheit 40 kommende Ergebnis wird über das Ergebnisregister 48 übertragen, und zwar über einen weiteren internen Bus 62, dem vom flüchtigen Speicher 16 über ein Speicherregister 18 sowie vom zweiten Schreib-/Lese-Speicher 78 Daten zugeführt werden, die Operanden darstellen.

Außerdem wird dem zweiten Schreib-/Lese-Speicher 78 über den Bus 62 das Ergebnis einer in der Recheneinheit 40 durchgeführten Rechnung zugeführt. Da zum zweiten Schreib-/Lese-Speicher 78 sowohl die zusätzliche Recheneinheit 40 (über den Bus 62) als auch der Mikroprozessor 90 (über den Datenbus 980) Zugriff haben, können über diesen zweiten Schreib-/Lese-Speicher 78 auch Daten zwischen der Recheneinheit 40 und dem Mikroprozessor 90 ausgetauscht werden.

Der interne Bus 62 dient, wie bereits erwähnt, im wesentlichen lediglich zum Übertragen von Daten. Da die Recheneinheit 40 auch Operationen mit mehrere Byte langen Operanden durchführen soll, ist der Datenbus 62 für eine größere Datenbreite ausgelegt, zum Beispiel für vier Byte. In diesem Zusammenhang wird davon ausgegangen, dass der erste Schreib-/Lese-Speicher 76 auch vier Byte parallel abgeben kann, entweder durch entsprechenden Aufbau oder durch eine interne Serien-Parallel-Umsetzung, die mehrere Wörter von einem Byte Länge nacheinander aufnimmt und parallel ausgibt. Eine entsprechende Anordnung ist mit dem Speicherregister 18 am Ausgang des flüchtigen Speichers 16 angedeutet, das also vier nacheinander zugeführte Byte parallel über den Bus 62 weiterleitet.

Die drei Operandenregister 42, 44, 46 sind so ausgelegt, dass sie vier Byte parallel aufnehmen sowie parallel oder gegebenenfalls in kleineren Abschnitten von weniger als vier Byte abgeben können, und zwar in Abhängigkeit davon, welche Wortlänge die zusätzliche Recheneinheit 40 verarbeiten kann. Das Ergebnisregister 48 für die Rechenergebnisse kann ebenfalls entsprechend dem Aufbau der Recheneinheit 40 mehrere Byte nacheinander oder parallel aufnehmen und jeweils vier Byte parallel über den internen Bus 62 übertragen.

Die Übertragung der Adressen von der zusätzlichen Recheneinheit 40 aus für den flüchtigen Speicher 16 sowie für den ersten Schreib-/Lese-Speicher 76 ist in Figur 5 aus Gründen der Übersichtlichkeit der Darstellung nicht näher gezeigt, denn die Adressierung von Speichern ist dem Fachmann wohlbekannt.

Schließlich sei in bezug auf die vorliegende Erfindung angemerkt, dass die fünf Register (vgl. Figuren 2 und 4), die in jedem Satz von Registern vorhanden sind, beispielsweise den folgenden Zwecken dienen können:

- Enthalten des Operationscodes zum Steuern der Recheneinheit 40;
- Angeben der Startadresse für den ersten Operanden;
- Enthalten der Startadresse für den zweiten Operanden;
- Enthalten der Adresse für einen weiteren Operanden, der in Abhängigkeit von der mit der Recheneinheit 40 auszuführenden Operation in unterschiedlicher Weise in der Recheneinheit 40 verarbeitet wird; beispielsweise stellt der Operand, der durch diese Adresse angegeben ist, den Modul bei Modulo-Operationen dar;
- Enthalten einer Adresse für das Rechenergebnis der Recheneinheit 40;
- Angeben der Länge des ersten Operanden; und/oder
- Angeben der Länge des zweiten Operanden.

Mit der gemäß Figur 2 (= erstes Ausführungsbeispiel), gemäß Figur 4 (= zweites Ausführungsbeispiel) sowie gemäß Figur 5 (= vereinfachte Zusammenschau aus erstem Ausführungsbeispiel und zweitem Ausführungsbeispiel) beschriebenen Anordnung kann die Rechenleistung der Recheneinheit 40 in optimaler Weise ausgenutzt werden, denn während des Ausführens einer Berechnung unter Verwendung eines ersten Satzes von Registern kann der Mikroprozessor 90 die Register eines weiteren Satzes mit neuen Werten laden, und wenn die Recheneinheit 40 einen Satz Operanden vollständig verarbeitet und das Ergebnis abgegeben hat, kann der Mikroprozessor 90 mit einem Schritt den Inhalt der Bitstellen 51, 52, 53, 54 des Kontrollregisters 50 ändern, so dass die Adressen für neue Operanden sofort gültig werden und die Berechnung mit diesen Operanden ohne Wartezeit starten kann. Die Angabe der Operandenadressen durch Startadresse und Operandenlänge ermöglicht eine sehr einfache, schnelle und registersparende Adressierung der Operanden.

BEZUGSZEICHENLISTE

100	Datenverarbeitungseinrichtung (erstes Ausführungsbeispiel; Fig. 2)
100'	Datenverarbeitungseinrichtung (zweites Ausführungsbeispiel; Fig. 4)
10	insbesondere peripherer Speicher
12	weitere Register
14	weitere Adressregister
16	flüchtiger Speicher
18	Speicherregister
20	erstes temporäres Register
22	zweites temporäres Register
24	drittes temporäres Register
26	viertes temporäres Register
28	fünftes temporäres Register
30	erstes Hauptregister
32	zweites Hauptregister
34	drittes Hauptregister
36	viertes Hauptregister
38	fünftes Hauptregister
40	(zusätzliche) Recheneinheit
42	erstes Operandenregister
44	zweites Operandenregister
46	drittes Operandenregister
48	Ergebnisregister
50	Kontrollregister
51	erste Bitstelle des Kontrollregisters 50
52	zweite Bitstelle des Kontrollregisters 50
53	dritte Bitstelle des Kontrollregisters 50
54	vierte Bitstelle des Kontrollregisters 50
55	fünfte Bitstelle des Kontrollregisters 50

56 sechste Bitstelle des Kontrollregisters 50

57 siebte Bitstelle des Kontrollregisters 50

58 achte Bitstelle des Kontrollregisters 50

59 neunte Bitstelle des Kontrollregisters 50

60 Kontrolllogik

62 interner (Operanden-)Bus

70 Adressregister

72 Zählregister

74 Auswahlschaltung

76 erster Schreib-/Lese-Speicher

78 zweiter Schreib-/Lese-Speicher

80 erstes dem Mikroprozessor 90 zugeordnetes Register

82 zweites dem Mikroprozessor 90 zugeordnetes Register

84 drittes dem Mikroprozessor 90 zugeordnetes Register

86 viertes dem Mikroprozessor 90 zugeordnetes Register

88 fünftes dem Mikroprozessor 90 zugeordnetes Register

90 Mikroprozessor

120 Datenbus vom Speicher 10 zu den temporären Registern 20, 22, 24, 26, 28

170 Beaufschlagen des Speichers 10 durch das Adressregister 70

230 Verbindung zwischen dem ersten temporären Register 20 und dem ersten Hauptregister 30

232 Verbindung zwischen dem zweiten temporären Register 22 und dem zweiten Hauptregister 32

234 Verbindung zwischen dem dritten temporären Register 24 und dem dritten Hauptregister 34

236 Verbindung zwischen dem vierten temporären Register 26 und dem vierten Hauptregister 36

238 Verbindung zwischen dem fünften temporären Register 28 und dem fünften Hauptregister 38

460 Verbindung zwischen der Recheneinheit 40 und der Kontrolllogik 60

	560	Verbindung zwischen dem Kontrollregister 50 und der Kontrolllogik 60
	670	Verbindung zwischen der Kontrolllogik 60 und dem Adressregister 70
	672	Verbindung zwischen der Kontrolllogik 60 und dem Zählregister 72
	980	interner Datenbus vom Mikroprozessor 90 zu den Registern 80, 82, 84, 86, 88
5	C	Recheneinheit gemäß dem Stand der Technik
	D	Datenverarbeitungseinrichtung gemäß dem Stand der Technik
	K	Kontrollregister gemäß dem Stand der Technik
	R1	erstes Register gemäß dem Stand der Technik
	R2	zweites Register gemäß dem Stand der Technik
10	R3	drittes Register gemäß dem Stand der Technik
	R4	viertes Register gemäß dem Stand der Technik
	R5	fünftes Register gemäß dem Stand der Technik
	S	Auswahlschaltung gemäß dem Stand der Technik

15

PATENTANSPRÜCHE

1. Datenverarbeitungseinrichtung (100; 100') mit mindestens einem Mikroprozessor (90) und mit mindestens einer zusätzlichen Recheneinheit (40) zum Durchführen mindestens einer bestimmten festgelegten Berechnung, wobei die Recheneinheit (40) mit dem Mikroprozessor (90) über eine Anzahl von Registern gekoppelt ist, von denen erste Register zum Steuern der Datenübertragung und zweite Register zum Übertragen von Befehlen vorgesehen sind,
dadurch gekennzeichnet,
dass die Register aus mindestens einem insbesondere peripheren Speicher (10), zum Beispiel
- aus mindestens einem R[andom]A[ccess]M[emory]-Speicher,
- aus mindestens einem R[ead]O[nly]M[emory]-Speicher oder
- aus mindestens einem E[lectrical] E[rasable] P[rogrammable] R[ead] O[nly] M[emory]-Speicher,

ladbar sind.

2. Datenverarbeitungseinrichtung gemäß Anspruch 1,
dadurch gekennzeichnet,
dass dem Speicher (10) mindestens ein Satz temporärer Register (20, 22, 24, 26, 28) zugeordnet ist, der mit mindestens einem der Recheneinheit (40) zugeordneten, zum Speichern der Register für die aktive Berechnung bestimmten Satz von Hauptregistern (30, 32, 34, 36, 38) in Verbindung (230, 232, 234, 236, 238) steht.

3. Datenverarbeitungseinrichtung gemäß Anspruch 1 oder 2,
dadurch gekennzeichnet,
dass der Speicher (10) durch mindestens ein zum Zeigen auf die Startadresse der zu ladenden Daten bestimmtes Adressregister (70) beaufschlagbar (170) ist, das mit mindestens einer Kontrolllogik (60) in Verbindung (670) steht.

4. Datenverarbeitungseinrichtung gemäß Anspruch 3,
dadurch gekennzeichnet,
dass der Recheneinheit (40) mindestens ein Kontrollregister (50) zugeordnet ist, das mit der Kontrolllogik (60) in Verbindung (560) steht.

5. Datenverarbeitungseinrichtung gemäß Anspruch 3 oder 4,
dadurch gekennzeichnet,
dass der Kontrolllogik (60) mindestens ein Zählregister (72) zum Angeben der in Folge zu ladenden Registersätze zugeordnet (672) ist.

6. Datenverarbeitungseinrichtung (100') gemäß mindestens einem der Ansprüche 1 bis 5,
dadurch gekennzeichnet,
dass zwischen den Satz temporärer Register (20, 22, 24, 26, 28) und den Satz von Hauptregistern (30, 32, 34, 36, 38) mindestens eine Auswahlschaltung (74) zum Kombinieren mit mindestens einem Satz (a, b, c) von dem Mikroprozessor (90) zugeordneten Registern (80, 82, 84, 86, 88) geschaltet ist.

7. Datenverarbeitungseinrichtung gemäß Anspruch 6,
dadurch gekennzeichnet,
dass die Auswahlschaltung (74) von mindestens einer Bitstelle (51, 52, 53, 54) des Kontrollregisters (50) beaufschlagbar ist.

8. Tragbarer Datenträger mit mindestens einer Datenverarbeitungseinrichtung (100; 100') gemäß mindestens einem der Ansprüche 1 bis 7.

9. Halbleiterchip mit mindestens einer integrierten Datenverarbeitungseinrichtung (100; 100') gemäß mindestens einem der Ansprüche 1 bis 7.

10. Verfahren zum Durchführen mindestens einer bestimmten festgelegten Berechnung mittels mindestens einer Datenverarbeitungseinrichtung (100; 100') mit mindestens einem Mikroprozessor (90) und mit mindestens einer zusätzlichen Recheneinheit (40), gekennzeichnet durch

die folgenden Verfahrensschritte:

(i) Initialisieren mindestens eines Adressregisters (70) und mindestens eines Zählregisters (72) durch den Mikroprozessor (90);

(ii) Starten der Berechnung durch Setzen mindestens eines Kontrollbits;

(iii) Kopieren bzw. Laden von bei der Startadresse beginnenden Daten aus mindestens einem insbesondere peripheren Speicher (10) in mindestens einen Satz temporärer Register (20, 22, 24, 26, 28);

(iv) Inkrementieren des Adressregisters (70) bei jedem Zugriff auf den Speicher (10);

(v) Feststellen, ob der Satz temporärer Register (20, 22, 24, 26, 28) vollständig ist:

(v.a) falls der Satz temporärer Register (20, 22, 24, 26, 28) vollständig ist (+), Gehen zu Verfahrensschritt (vi);

(v.b) falls der Satz temporärer Register (20, 22, 24, 26, 28) nicht vollständig ist (-), Gehen zu Verfahrensschritt (iii);

(vi) Feststellen, ob die Recheneinheit (40) aktiv ist:

(vi.a) falls die Recheneinheit (40) aktiv ist (+), Gehen vor Verfahrensschritt (vi);

(vi.b) falls die Recheneinheit (40) nicht aktiv ist (-), Gehen zu Verfahrensschritt (vii);

(vii) Kopieren bzw. Übertragen der Daten vom Satz temporärer Register (20, 22, 24, 26, 28) in mindestens einen Satz von Hauptregistern (30, 32, 34, 36, 38);

(viii) Dekrementieren des Zählregisters (72);

(ix) Starten der Berechnung in der Recheneinheit (40);

(x) Feststellen, ob das Zählregister (72) auf Null dekrementiert ist:

(x.a) falls das Zählregister (72) auf Null dekrementiert ist (+), Gehen zu Verfahrensschritt (xi);

(x.b) falls das Zählregister (72) nicht auf Null dekrementiert ist (-), Gehen zu Verfahrensschritt (iii);

(xi) Beenden.

ZUSAMMENFASSUNG

Datenverarbeitungseinrichtung mit Mikroprozessor und mit zusätzlicher Recheneinheit sowie zugeordnetes Verfahren

Um eine Datenverarbeitungseinrichtung (100; 100') mit mindestens einem Mikroprozessor (90) und mit mindestens einer zusätzlichen Recheneinheit (40) sowie ein Verfahren zum Durchführen mindestens einer bestimmten festgelegten Berechnung mittels der Datenverarbeitungseinrichtung (100; 100') so weiterzuentwickeln, dass eine Vielzahl von Berechnungen in Folge ohne Eingreifen des Mikroprozessors (90) durchgeführt werden kann, wird vorgeschlagen, dass die Register aus mindestens einem insbesondere peripheren Speicher (10), zum Beispiel

- aus mindestens einem R[andom]A[ccess]M[emory]-Speicher,
- aus mindestens einem R[ead]O[nly]M[emory]-Speicher oder
- aus mindestens einem E[lectrical] E[rasable] P[rogrammable] R[ead] O[nly] M[emory]-Speicher,

ladbar sind.

Fig. 2

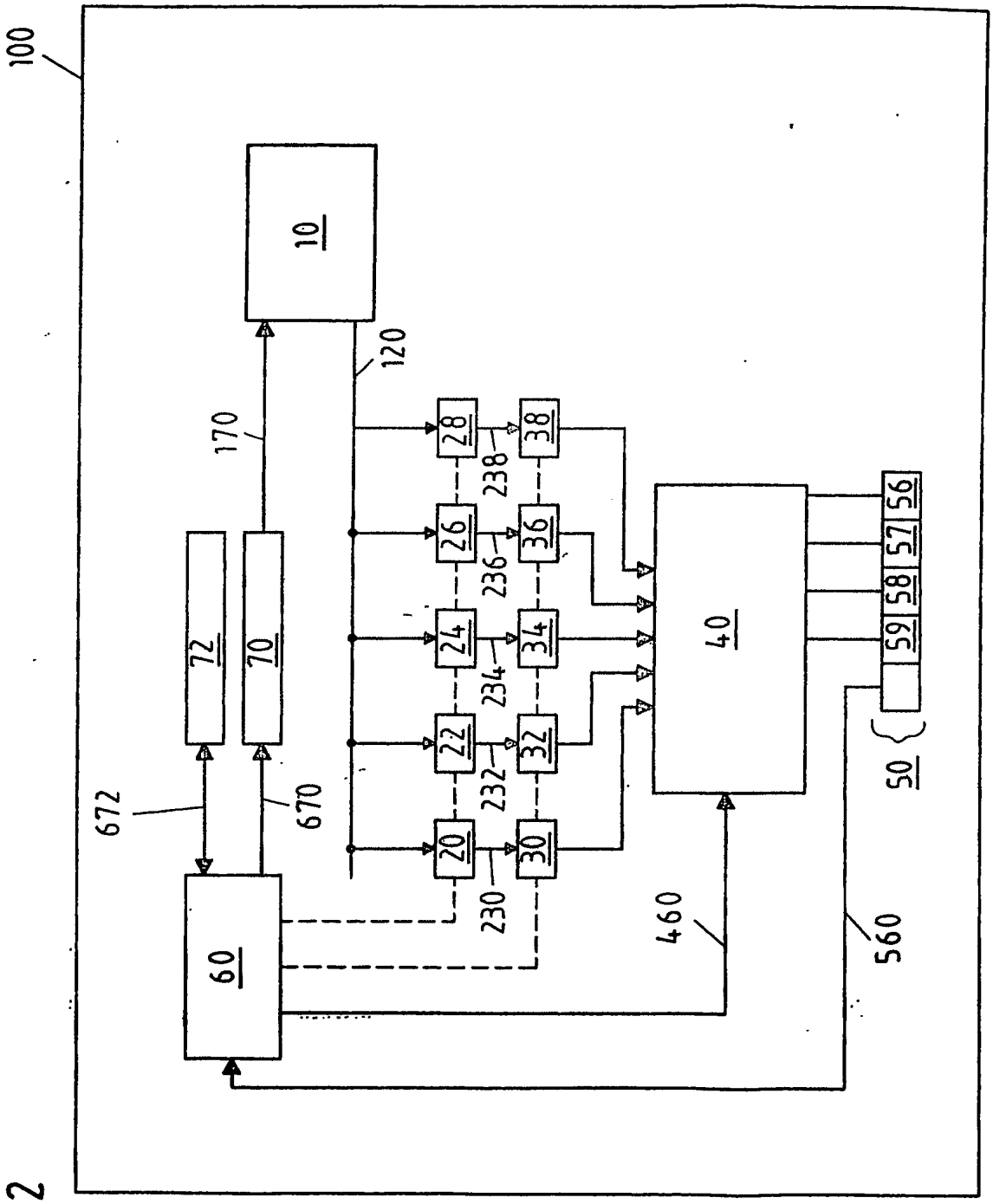

100
10
120
170
28
38
238
26
36
236
24
34
234
22
32
232
20
30
230
72
70
672
670
60
40
56
57
58
59
50
460
560

Fig.2

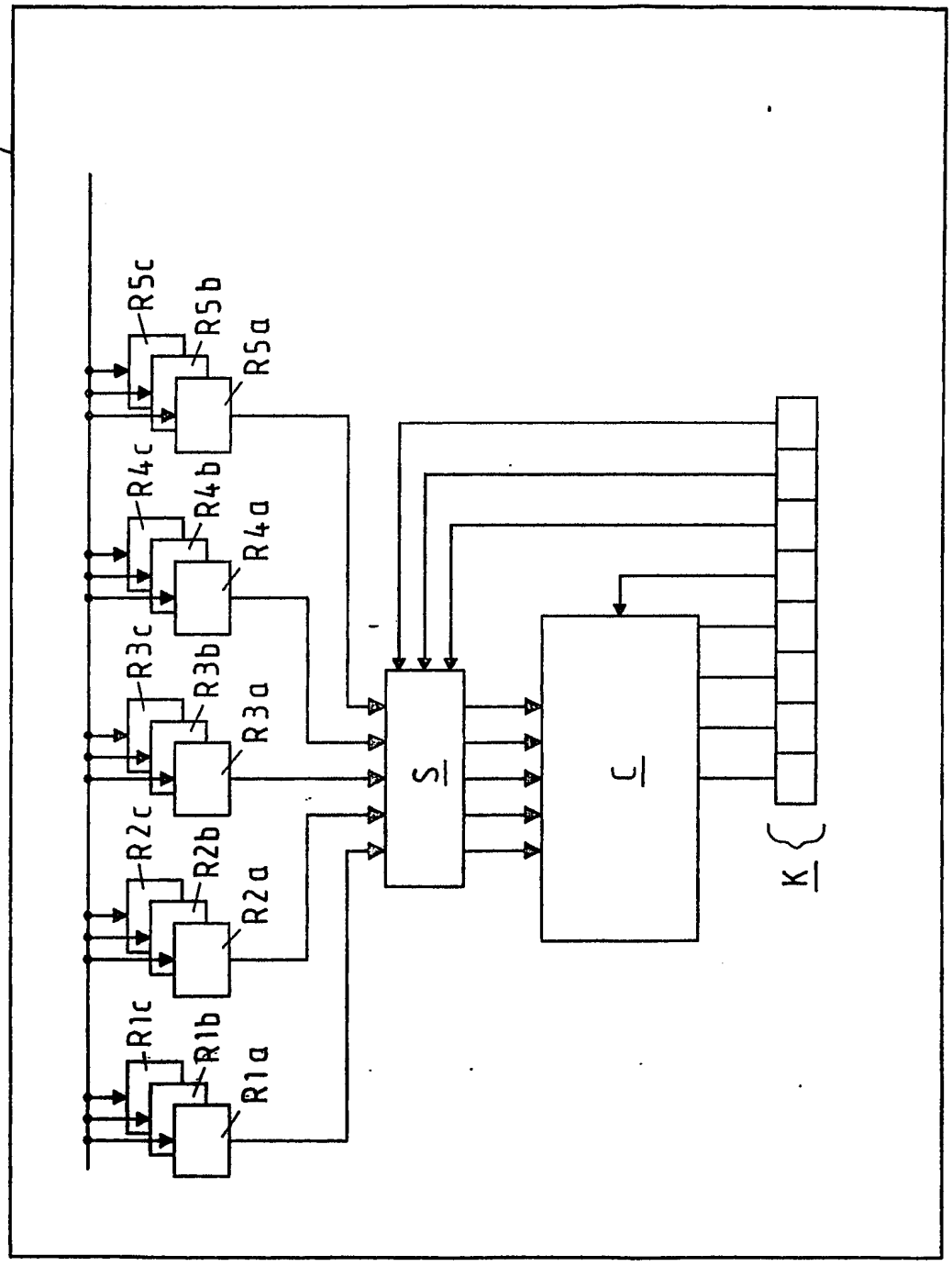


Fig.1

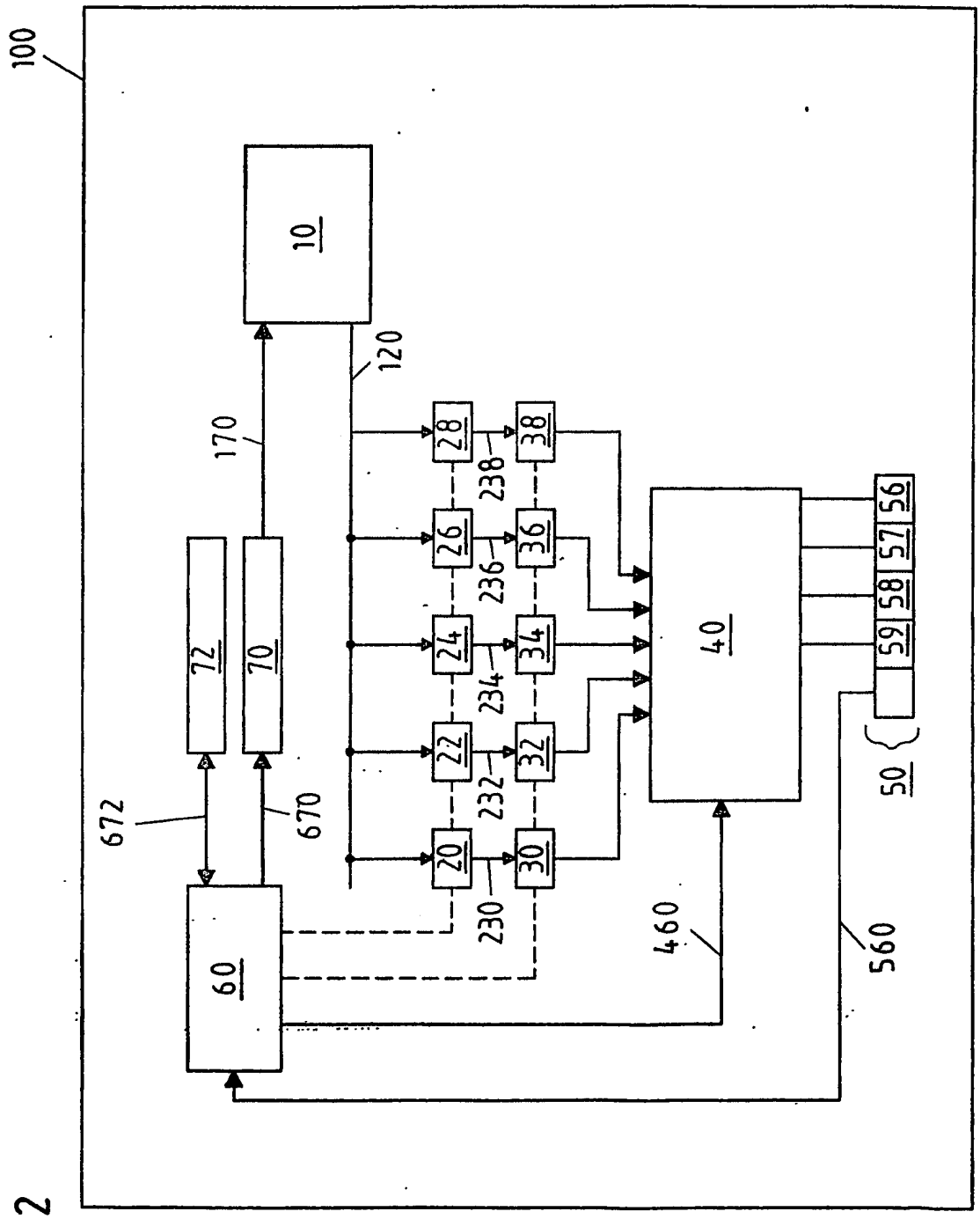
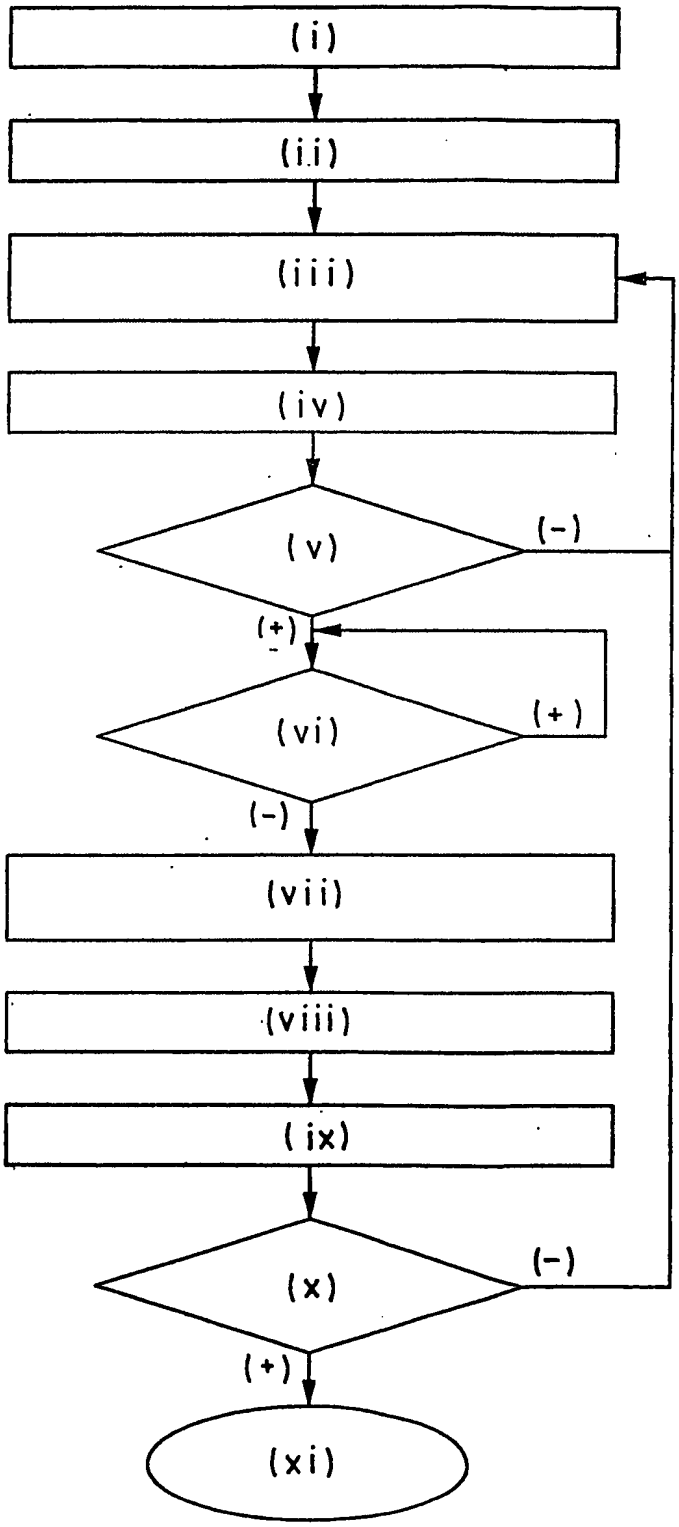

100
10
120
170
28
38
238
26
36
236
24
34
234
22
32
232
20
30
230
72
70
672
670
60
40
460
56
57
58
59
50
560

Fig. 2

Fig.3



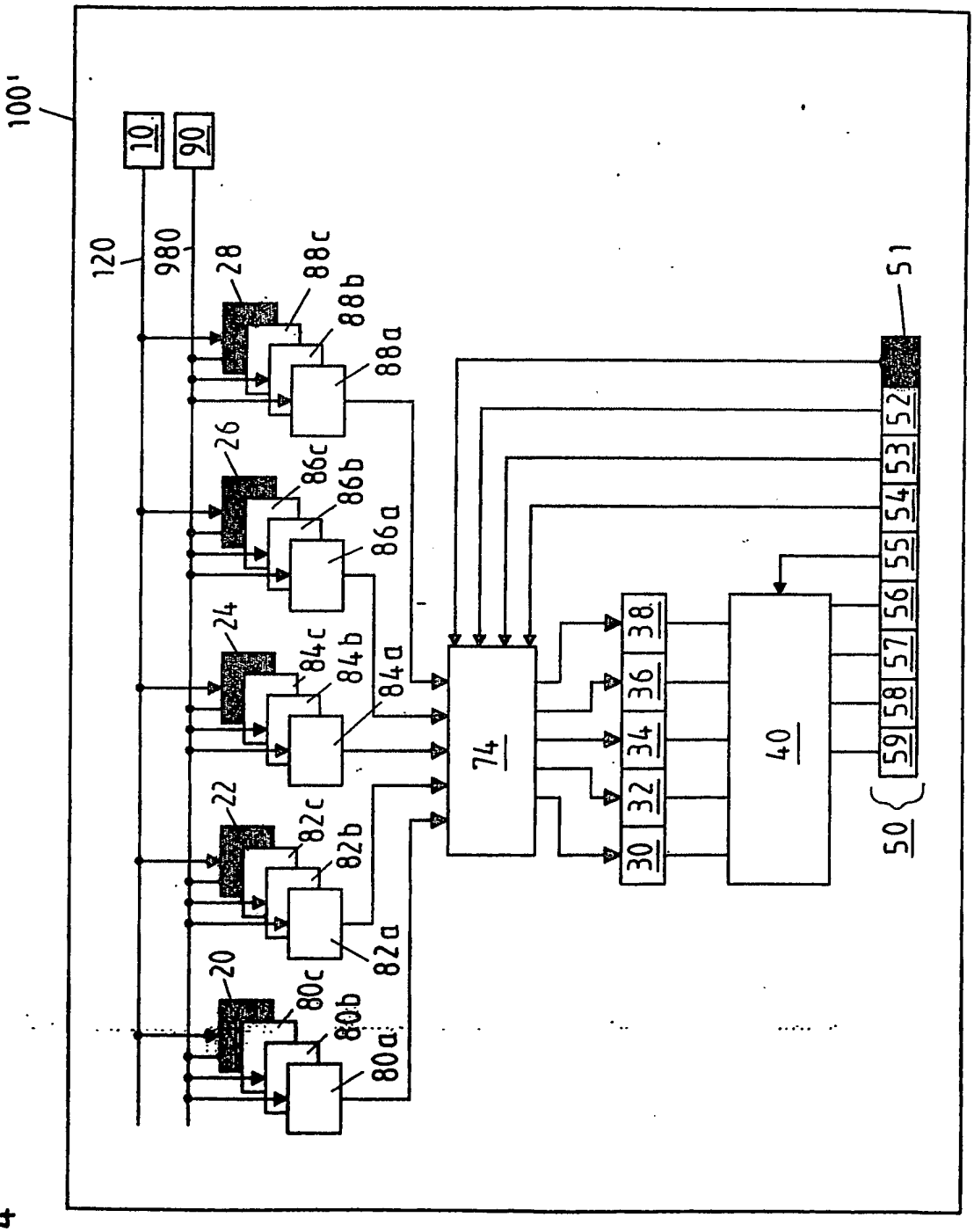

100'
10
90
120
980
28
88c
88b
88a
26
86c
86b
86a
24
84c
84b
84a
22
82c
82b
82a
20
80c
80b
80a
74
40
51
52
53
54
55
56
57
58
59
50
38
36
34
32
30

Fig. 4

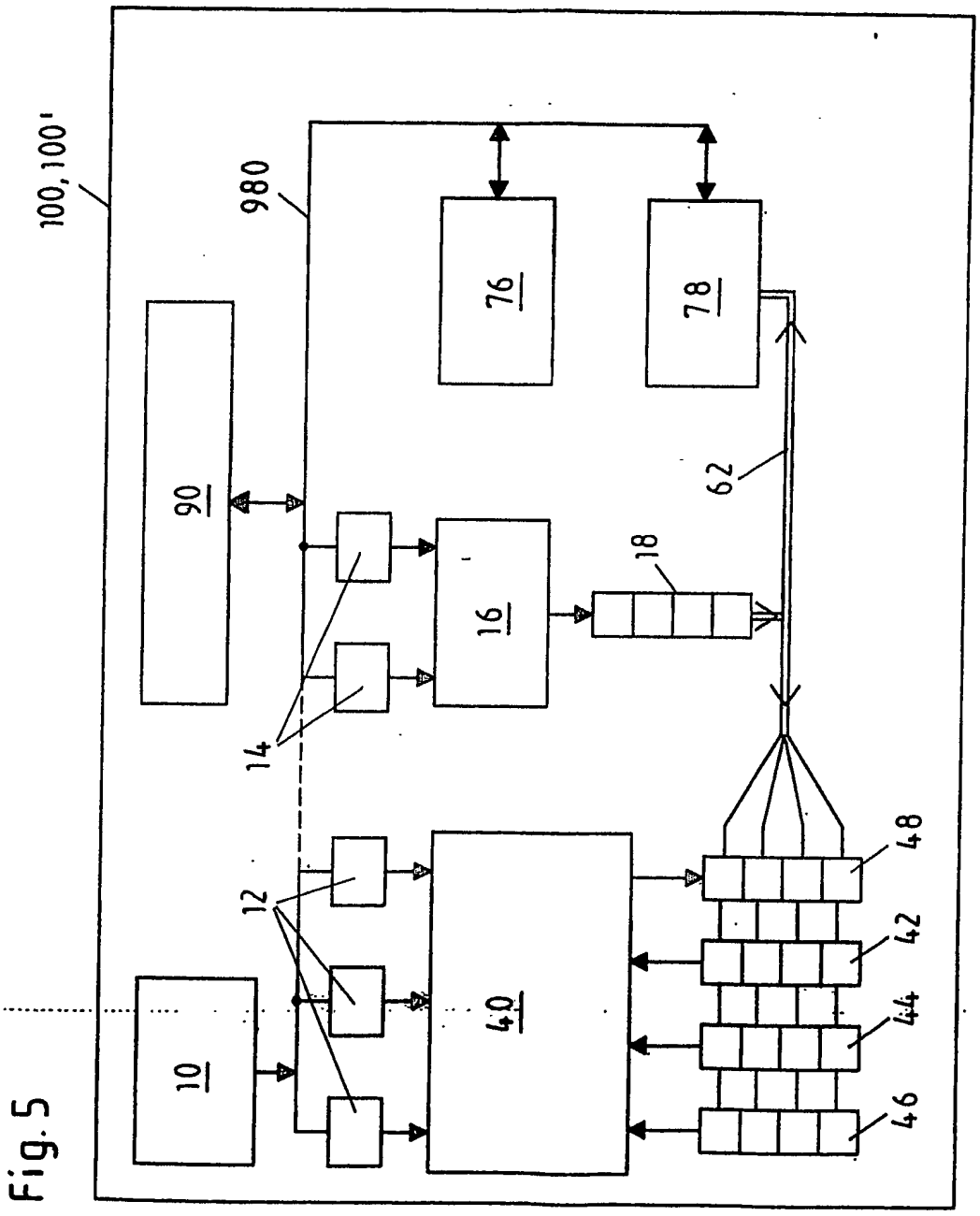


Fig.5